Implementation of Virtual Firewall Mechanism for Security of Indonesian E-Health Cloud Model

Sarah Syahwenni Utari [1], Sri Chusri Haryanti [1], Ummi Azizah Rachmawati [1],
Sri Puji Utami Atmoko [1], Heru Suhartanto[2]
[1]Faculty of Information Tecnology, Universitas YARSI, Indonesia
[2]Faculty of Computer Science, Universitas Indonesia
sarahsyahweni@gmail.com[1]; sri.chusri@yarsi.ac.id[1]; ummi.azizah@yarsi.ac.id[1]; puji.atmoko@yarsi.ac.id[1]; heru@cs.ui.ac.id[2]

Abstract

Cloud computing is a new paradigm in using resources and providing computing services. Adoption of cloud computing in e-health is expected to be able to improve health services and help research in health services. There has been a proposal of e-health cloud deployment model for Indonesia. However, there need to be stages of works on cloud computing adoption for e-Health services before implementation decisions. One of the considerations in cloud computing is security. In this work, we examine the implementation of virtual firewall mechanism for Indonesian e-health cloud model from DDoS attack. Proxmox VE is used in the virtualization environment of Indonesian e-Health cloud model, and the ConfigServer & Firewall (CSF) is modified. DDoS-blocking script is used to block IPs from attackers. The inspection is done in two scenarios. The purpose of the first scenario is to find out the average time of a server cloud bear up in a DDoS attack. The second scenario is done to verify the virtual firewall capability. The result obtained from the first scenario is that the average time is 197.26 seconds with the standard deviation is 52.99 seconds before a server was down because of DDoS attacks. The results of the second scenario show that virtual firewall managed to block the attacker IP address and the server could withstand from DDoS attacks.

Keywords: *DDoS Attack, e-health cloud, virtual firewalls.*

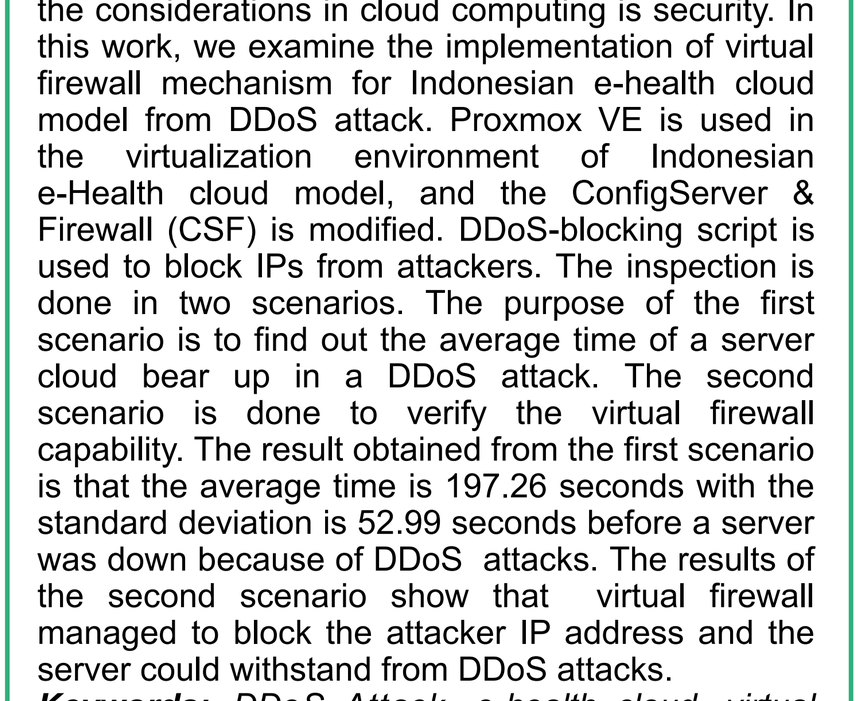

Figure 1. Indonesian e-Health Community Cloud Model [1]

Pseudocode of IP Address Filtering

```
If (Client require Server)
   Client IP address is filtered by CSF
      At CSF
Step 1: Identification of incoming client
      If (Client IP address is not found in /etc/csf/csf.allow (Client IP))
         ADD Client IP to /etc/csf/csf.allow (Client IP)
      Else If (/etc/csf/csf.allow (same Client IP) > N [within session BAN_PERIOD])
         MOVE Client IP to /var/log/ddos.log
         BLACKLISTED use ddos-blocking.sh filtered at ddos-blocking.conf
         Alert DDoS Attack
      Else
         Client IP address is found in /etc/csf/csf.deny (Client IP))
         can't access to Server.
Step 2 : Monitoring the request rate
      If (for any Client IP (REQUEST < = MAX_PACKET))
         Forward Client IP to csfposh.sh to PROTECTED SERVER
      Else
         MOVE Client IP to /var/log/ddos-blocking.log
         BLACKLISTED use ddos-blocking.sh filtered at ddos-blocking.conf
         Alert DDoS Attack.
```

Figure 2. Pseudocode of IP Address Filtering

Topology

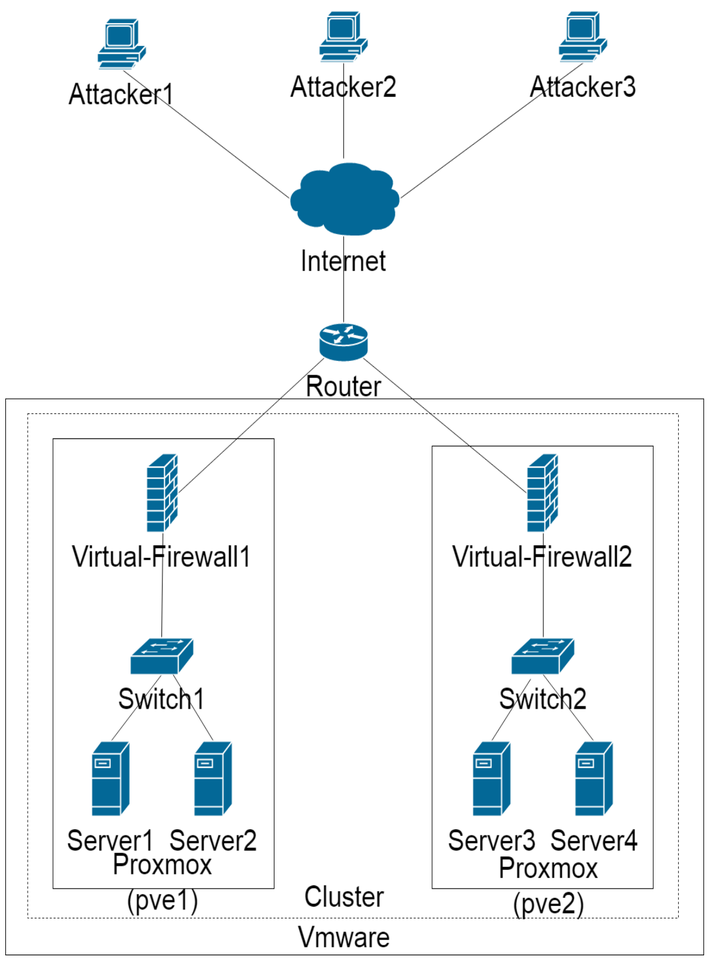

Figure 3. Indonesian e-Health Cloud Network Topology

Hardware and Software Specification

Nodes	Virtual Router	Virtual Server	Attackers
OS : Proxmox VE 4.4	OS : Ubuntu Server 14.04	OS : Ubuntu Server 14.04	OS : Kali Linux 2017
Processors : 4	Memory : 512 MB	Memory : 512 MB	Memory : 1 GB
Memory : 5.9 GB	Processors : 1	Hard Disk 8 GB (local-lvm)	Hard Disk (IDE) : 20 GB
Hard Disk (IDE) : 100 GB	Hard Disk : 8 GB (local-lvm)	Network Adapter 1 : Bridge (vmbr2)	Network Adapter1 : Custom (VMnet2)
Network Adapter1 : Custom (VMnet2)	Network Adapter1 : Bridge (vmbr1)		
Network Adapter2 : Custom (VMnet2)	Network Adapter2 : Bridge (vmbr2)		
Network Adapter3 : Custom (VMnet3)			

Table 1. Hardware and Software Specification

Experiments

There are two scenarios applied. The first is performed to find out the average number of packets received by the server, the average and the standard deviation of downtime, also network traffic in the event of DDoS attacks. The second scenario intends to prove that the virtual firewall could manage to block the attacker IP address.

Result

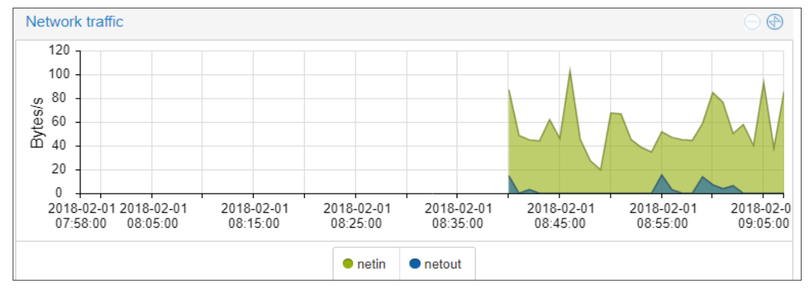

Figure 4. Traffic Network of 1st Scenario

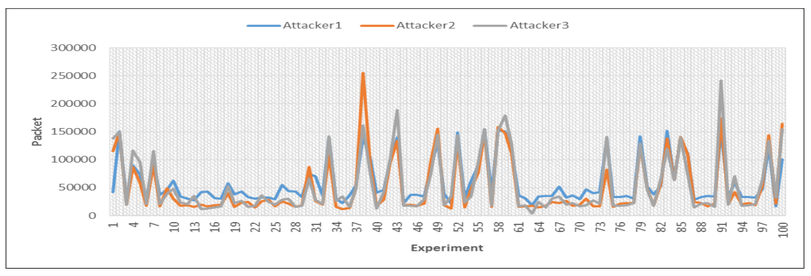

Figure 5. Graph of Attack on 1st Scenario

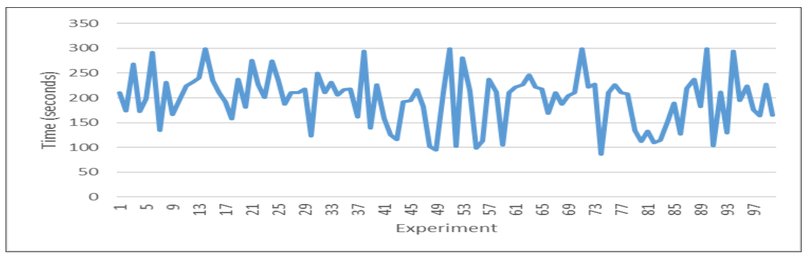

Figure 6. Downtime Graph on 1st Scenario

In 2nd scenario, the attacker's IP address will be blocked resulting in a block list (Figure 7).

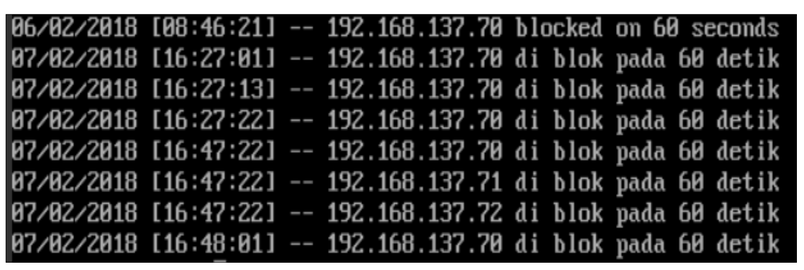

Figure 7. Block List IP Addresses

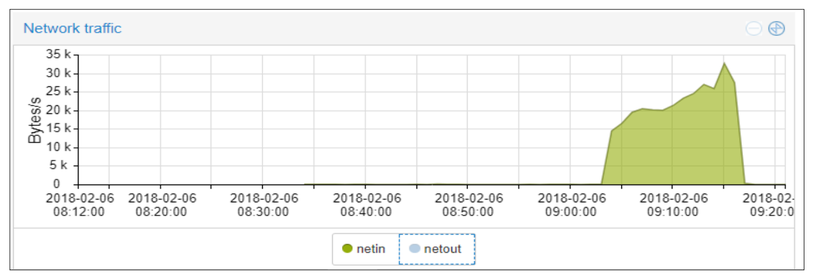

Figure 8. Traffic Network of 2nd Scenario

Conclusion

Virtual firewall by modifying CSF on Ubuntu 14.04 is working successfully for Indonesia e-health cloud model. Without modification of the CSF as a virtual firewall, average downtime obtained is 197.26 seconds with the standard deviation is 52.99 seconds. Virtual firewall managed to block the attacker IP address and the server could withstand from DDoS attacks.

Future Work

For further research, a security system can be designed to filter the DDoS attacks originating from within the network. In the future, the e-Health cloud security model would be tested in a testbed.

References

[1] Haryanti, S. C., Pradipta, A., Atmoko, S. P. U., Rachmawati, U. A., Suhartanto, H. (2017). *Indonesian E-Health Community Cloud*. Poster, SEAIP 4-8 Desember 2017, Taiwan.
[2] Singh, B., Mahajan, R., Panda, S.N. and Samra, G.S., **2016**. *Detecting DDOS Attacks in Cloud-A Novel Approach*. International Journal of Computer Science and Information Security, 14(5), p.292.
[3] Al Nuaimi, N., AlShamsi, A., Mohamed, N., & Al-Jaroodi, J. (**2015**, March). *e-Health cloud implementation issues and efforts. In Industrial Engineering and Operations Management* (IEOM), 2015 International Conference on (pp. 1-10). IEEE.
[4] Ahmed, E.S.A. and Elatif, R.E., **2015**. *Network denial of service threat security on cloud computing a survey*. International Journal of Scientific Research in Science, Engineering and Tecnology, 1(5), pp. 341-50.
[5] Islam, T., Manivannan, D., & Zeadally, S. (2016). *A classification and characterization of security threats in cloud computing*. Int. J. Next-Gener. Comput, 7(1).
[6] Mishra, A., dkk. (2013). *Cloud Computing Security. International Journal on Recent and Innovation Trends in Computing and Communication, 36-39*(1).